J Cryptol (2024) 37:34
https://doi.org/10.1007/s00145-024-09515-4

Journal of
CRYPTOLOGY

Research Article

Randomness Recoverable Secret Sharing Schemes

Mohammad Hajiabadi
University of Waterloo, Waterloo, Canada
mdhajiabadi@uwaterloo.ca

Shahram Khazaei · Behzad Vahdani
Sharif University of Technology, Tehran, Iran
shahram.khazaei@sharif.ir
vahdani.behzad@proton.me

Communicated by Svetla Nikova

Received 3 July 2023 / Revised 17 July 2024 / Accepted 18 July 2024

Abstract. It is well-known that randomness is essential for secure cryptography. The randomness used in cryptographic primitives is not necessarily recoverable even by the party who can, e.g., decrypt or recover the underlying secret/message. Several cryptographic primitives that support randomness recovery have turned out useful in various applications. In this paper, we study *randomness recoverable secret sharing schemes* (RR-SSS), in both information-theoretic and computational settings and provide two results. First, we show that while every access structure admits a perfect RR-SSS, there are very simple access structures (e.g., in monotone AC^0) that do not admit efficient perfect (or even statistical) RR-SSS. Second, we show that the existence of efficient computational RR-SSS for certain access structures in monotone AC^0 implies the existence of one-way functions. This stands in sharp contrast to (non-RR) SSS schemes for which no such results are known. RR-SSS plays a key role in making advanced attributed-based encryption schemes randomness recoverable, which in turn have applications in the context of designated-verifier non-interactive zero knowledge.

Keywords. Secret sharing, Randomness recovery, Lower bounds, Information theoretic security, Randomness recoverable attribute based encryption, One way function.

1. Introduction

Without randomness, secure cryptography is unachievable. The randomness used in cryptographic primitives is not necessarily, efficiently and even sometimes information-theoretically, recoverable. For example, the randomness used for an ElGamal ciphertext is not efficiently recoverable even by a party holding the secret key. On the other hand, several well-known constructions for PKE, such as the OAEP [7] and its variants [10,34, 37] are randomness recoverable (RR). Another notable RR-PKE construction is Yao's construction [39] based on injective trapdoor functions (TDF).

Published online: 20 August 2024

RR-PKE schemes have found applications in constructing optimistic fair exchange protocols [32], signcryption schemes [30], proofs of correct decryptions in electronic-voting applications in [26] (to avoid heavy zero-knowledge proofs) and recently in CCA-secure PKE in [16].

In addition to PKE, RR variants of symmetric encryption schemes (SKE), attribute-based encryption (ABE) and garbled circuits (GC) have been studied in the literature [15,27].

1.1. *RR Secret Sharing and Motivations*

In this paper, we initiate the study of secret sharing schemes (SSS) [9,36] from a randomness recovery point of view. In addition to being an interesting notion on its own, it has applications in settings such as designated-verifier non-interactive zero-knowledge (DV-NIZK) for NP [15,31], as we will discuss later.

Main Results We take the first steps toward delineating the notion of RR-SSS from both information-theoretic and computational perspectives. First, we show that while every access structure admits a perfect RR-SSS, there are very simple access structures (e.g., in AC^0) that do not admit efficient perfect RR-SSS. Our result also applies to the weaker security notions including *statistical security*. Second, we show that the existence of efficient computational RR-SSS for certain access structures in AC^0 implies one-way functions (OWF). Our second result provides strong evidence that realizing RR-SSS for AC^0 from assumptions not currently known to imply OWFs (e.g., worst-case complexity-type assumptions) may be impossible.

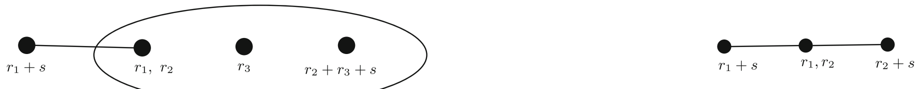
Applications of RR-SSS and Motivations Assuming the existence of RR-PKE, RR-SSS for access structures in NC^1 seems to be an important step towards single-key RR-ABE for circuits in P (see Sect. 1.5). Single-key RR-ABE for P, in turn, is sufficient for DV-NIZK for all NP [15,31][1]. Currently, it is known how to base RR-ABE and DV-NIZK on CDH and LWE [15,31] but it is still open whether they can be achieved using weaker primitives such as TDFs (which by [15] is implied by RR-PKE and hinting PRG [29]).

Moreover, RR-SSS can be useful in applications in which proofs of well-formedness are needed for recovered shares. This motivates the study of RR-SSS as an independent primitive.

1.2. *A Perfect RR-SSS for Every Access Structure*

Let us first recall what an SSS is. In an SSS, a secret is shared among a set of participants by giving a share to each one. The shares are computed by applying a public rule on the secret and randomness. Only certain pre-specified subsets of participants are *qualified* to recover the secret and the secret must remain hidden from every other subset of participants. These requirements are called *correctness* and *privacy*, respectively, and can be defined either in the computational or information-theoretic setting. The set of all qualified subsets is called the *access structure* [20].

[1] Lombardi et al. [31] showed how to generically construct DV-NIZK from single-key weak function-hiding ABE. These sorts of ABE can be constructed from single-key RR-ABE [15].



(a) A non-RR-SSS.

(b) A RR-SSS.

Fig. 1. The ISN1 construction is not randomness recoverable in general .

In an RR-SSS, we additionally require that every qualified set, in addition to the secret, is also able to recover the randomness.

The most well-known SSS, *Shamir's threshold scheme*, is RR. In Shamir's scheme, a secret $s \in \mathbb{F}$ is shared among a set of n participants as follows ($\mathbb{F}$ is a finite field with at least $n+1$ elements). The randomness $(r_1, \ldots, r_{t-1}) \in \mathbb{F}^{t-1}$ is chosen ($1 \le t \le n$), the polynomial $f(x) = s + r_1 x + r_2 x^2 + \ldots + r_{t-1} x^{t-1}$ is constructed, and the share $s_i = f(x_i)$ is given to participant $i \in \{1, \ldots, n\}$, where $x_1, \cdots, x_n$ are some distinct public elements of $\mathbb{F}$. It is easy to verify that only a subset A of size at least t is qualified to recover the secret using the shares $\{s_i\}_{i \in A}$. The corresponding access structure is called the (n, t)-*threshold access structure*. It is also easy to see that in Shamir's scheme, a qualified set recovers the polynomial $f(x)$, and hence, the randomness.

Not every SSS is RR. For example, consider the well-known Ito-Saito-Nishizeki construction in [20] for a general access structure, which we refer to as the *ISN1*. The secret is a single bit $s \in \mathbb{F}_2$ and the randomness is

$$\mathcal{R} = \{r_{A,i} \mid A \text{ is a minimal qualified set and } i \in A\},$$

where a qualified set is called *minimal* if none of its proper subsets are qualified. The $r_{A,i}$'s are randomly chosen bits subject to $\sum_{i \in A} r_{A,i} = s$. The share of a participant i is

$$s_i = \{r_{A,i} \mid \text{there exists a minimal qualified set } A \text{ such that } i \in A\} .$$

It is easy to verify that the construction is information-theoretically both correct and private. However, as shown in Fig. 1, the ISN1 construction is not RR in general.

A perfect RR-SSS construction A natural question to ask is whether every access structure admits a perfect (i.e., information-theoretically secure) RR-SSS. The answer to this question is not entirely trivial, but in the following, we show that another general construction, also introduced by Ito-Saito-Nishizeki in [19] which we refer to as the *ISN2*, is RR.

The secret is again a single bit $s \in \mathbb{F}_2$ and the randomness is

$$\mathcal{R} = \{r_B \mid B \text{ is a maximal unqualified set}\},$$

where an unqualified set is called *maximal* if every proper superset of it is qualified. The r_B's are randomly chosen bits. The share of a participant i is

$$s_i = \left(s + \sum_B r_B, \{r_B \mid B \text{ is a maximal unqualified set and } i \notin B\}\right) .$$

It is easy to verify that the construction is both perfectly correct and perfectly private. Also, a minimal qualified set recovers the whole randomness.

Fact 1.1. *The ISN2 construction [19] is RR.*

1.3. *Results on Perfect RR-SSS*

We study the RR variant of some questions that have been extensively studied for (standard) perfect SSSs.

On Beimel's conjecture for RR-SSSs The *information ratio*, defined to be the ratio between the largest share size and the secret size, is an important parameter that measures the efficiency of a SSS. Both ISN1 and ISN2 constructions have exponential information ratios in the number of participants. A long-standing open problem in the theory of secret sharing is to answer whether exponential upper bound is inevitable. Beimel [5] has conjectured that this is the case.

Conjecture 1.2. (Beimel) *There exists an $\varepsilon > 0$ such that, for every integer n, there is an access structure with n participants such that every perfect SSS that realizes it has information ratio $2^{\Omega(n^{\varepsilon})}$.*

Surprisingly, the best-known lower bound, due to Csirmaz [12], is $\Omega(n/\log n)$. We prove that an exponential lower bound holds for perfect RR-SSSs.

Theorem 1.3. (Exponential lower bound for perfect RR-SSS) *For every integer n, there is an access structure with n participants such that every perfect RR-SSS that realizes it has information ratio $2^{\Omega(n)}$.*

We prove the theorem for an access structure on n participants, which is the union of $n/3$ disjoint $(3, 3)$-threshold access structures (see Fig. 2); but the result holds in general, i.e., for the union of n/k disjoint (k, k)-thresholds for every $k \geq 2$. Similarly to Csirmaz, we use the so-called *Shannon-type information inequalities* to prove an exponential lower bound on the information ratio of this access structure for perfect RR-SSSs.

On weaker security notions Several non-perfect security notions for secret sharing have been proposed in the literature. It is well-known [22, Theorem 36] that any lower bound derived using information inequalities applies not only to perfect security but also to standard relaxations such as quasi-perfect [22, Chapter 5], almost-perfect [13,23], and statistical security. The exponential lower bound of Theorem 1.3 is also valid for these relaxations because we only use (Shannon-type) information inequalities in the proof.

Ruling out the existence of efficient perfect RR-SSS for mAC^0. Access structures are in 1-1 correspondence with monotone circuits. The mAC^0 class consists of all monotone circuits of depth $O(1)$ and polynomial size, with AND/OR gates with unbounded fan-in. Unfortunately, the above result shows that we cannot have efficient perfect RR-SSS for access structures even in mAC^0.

On contrary, the class of access structures admitting efficient perfect (standard) SSSs is much richer. In particular, it contains mNC^1, the class of monotone circuits of depth

$O(\log n)$ and polynomial size with AND/OR gates with a maximum fan-in of 2, which is known to strictly contain mAC^0. We refer to [6] for further discussion on the class of efficient perfect SSSs. It is open whether every access structure in mP, the class of monotone circuits of polynomial size with AND/OR gates with unbounded fan-in, admits an efficient perfect SSS.

1.4. *Results on Computational RR-SSS*

In a computational SSS [35], we require that the sharing and reconstruction algorithms be polynomial-time in the security parameter and the number of participants. Furthermore, we require that a polynomial-time adversary cannot distinguish between the shares of an unqualified set for every pair of secrets.

An unpublished result by Yao shows that assuming the existence of *one-way functions*, every access structure in mP admits an efficient computational SSS. The construction is a generalization of the results of Benaloh and Leichter [8] that constructs a perfect SSS for polynomial-size monotone formulae. We refer to [38] for details of the construction. In a recent work by Applebaum et al. [4], this result is extended to certain classes of access structures that lack efficient representation. By assuming OWFs with sub-exponential security, they construct computational secret sharing schemes with share sizes that are poly-logarithmic in the representation size of the access structure (which corresponds to the size of the truth table or the graph). It is open whether (efficient) computational SSS for any class of access structures implies OWFs. Assuming the existence of OWFs, an unpublished result of Rudich shows that computational SSS for mNP implies oblivious transfer; see [5,28].

OWFs from RR-SSS for AC^0 As we mentioned above, it is still open whether computational (standard) SSS for any class of access structures implies OWFs. One main obstacle to proving this possibly true statement is that the existence of efficient perfect SSS for every access structure has not yet been (unconditionally) ruled out, even though it is generally believed not to be the case, as it has been manifested in Beimel's conjecture (Conjecture1.2). However, by our result on the exponential lower bound for RR-SSS (Theorem 1.3), the situation for RR-SSS is different. We use the method developed by Impagliazzo and Luby in [18], together with a variant of Csirmaz's framework [12] for lower bounding the information ratio of perfect SSSs adapted for the computational setting, to prove that existence of computational RR-SSS for certain access structures in AC^0 implies the existence of OWFs.

Construction of computational RR-SSS A perfect linear SSS can be converted into a computational RR-SSS using a one-time KDM-secure SKE naturally and straightforwardly. For the sake of completeness, in Sect. 5, we state this formally. In that section, we introduce a type of PRG with a KDM-like security which turns out convenient in constructing a simple computational RR-SSS from a perfect linear SSS with the same access structure.

1.5. *Applications of RR-ABE*

The notion of RR-SSS was implicitly used as a key tool to obtain randomness recoverable single-key attribute-based public-key encryption schemes [15,31], which in turn imply

DV-NIZK for all NP [31]. Let us recall the definition of ABE. We have a master public key mpk and a master secret key msk. For any attribute string x, we have an attribute secret key sk_x, obtained as $\mathsf{KGen}(msk, x)$, where KGen is the key generation algorithm of the ABE. We encrypt a message m under mpk and a given circuit C to get a ciphertext ct. Now someone who has sk_x can decrypt ct to get m iff $C(x) = 1$.

We say that the ABE is RR if when $C(x) = 1$, then sk_x not only recovers m, but also all the randomness used by the encryption algorithm.

In the single-key security notion, an adversary can ask for only one attribute secret key sk_x, and has to win in an indistinguishability sense against a challenger who encrypts with respect to some circuit C where $C(x) = 0$.

A standard way to build single-key RR-ABE is as follows: if $|x| = n$, then the master secret key has n PKE secret keys $(sk_1, ..., sk_n)$ and mpk contains the corresponding public keys $(pk_1, ..., pk_n)$. An attribute secret key for x contains those sk_i where $x_i = 1$. To encrypt m under mpk and C, we share m according to C to get the shares. We then encrypt each share under pk_i, and return all the ciphertexts. The notion of RR-SSS is a key tool in realizing randomness recoverability for the above single-key ABE scheme, as it allows us to recover the randomness used by sharing process, a major source of the overall randomness.

2. Preliminaries

In this section, we present the necessary background.

2.1. *Random Variables*

We denote random variables (RV) by boldface characters and use $\mathsf{supp}(\boldsymbol{X})$ to denote the support of RV $\boldsymbol{X}$. We use the terms RV and distribution interchangeably throughout the paper. The Shannon entropy of $\boldsymbol{X}$ is denoted by $\mathrm{H}(\boldsymbol{X})$. The entropy of $\boldsymbol{X}$ conditioned on RV $\boldsymbol{Y}$ is denoted and defined by $\mathrm{H}(\boldsymbol{X}|\boldsymbol{Y}) := \mathrm{H}(\boldsymbol{X}, \boldsymbol{Y}) - \mathrm{H}(\boldsymbol{Y})$. The mutual information between $\boldsymbol{X}, \boldsymbol{Y}$ is defined and denoted by $\mathrm{I}(\boldsymbol{X} : \boldsymbol{Y}) := \mathrm{H}(\boldsymbol{X}) - \mathrm{H}(\boldsymbol{X}|\boldsymbol{Y})$.

Let us also recall the *functional representation lemma* [14, page 626], a well-known lemma in information theory, that will be used in this paper. We use the notation $\boldsymbol{X} \equiv \boldsymbol{Y}$ for identically distributed RVs.

Lemma 2.1. (Functional representation lemma [14]) *For every pair of jointly distributed RVs* $(\boldsymbol{X}, \boldsymbol{Y})$*, there exists a RV* $\boldsymbol{R}$*, independent of* $\boldsymbol{X}$*, and a mapping* μ *such that* $(\boldsymbol{X}, \boldsymbol{Y}) \equiv \big(\boldsymbol{X}, \mu(\boldsymbol{X}, \boldsymbol{R})\big)$

Remark 2.2. Throughout the paper, we will consider a *non-uniform* model of computation, however, our results hold true for the *uniform* model.

We call the family $\boldsymbol{X} = \{\boldsymbol{X}_\lambda\}_{\lambda \in \mathbb{N}}$ of RVs *efficiently sampleable* if there exists a family of polynomial-time algorithms $\mathsf{Sample} = \{\mathsf{Sample}_\lambda\}_{\lambda \in \mathbb{N}}$ such that $\mathsf{Sample}_\lambda(1^\lambda) \equiv \boldsymbol{X}_\lambda$. We call λ the *security parameter* and refer to $\boldsymbol{X}$ as a *family of RVs*, or simply an RV, indexed by the security parameter. We recall that a function $\varepsilon : \mathbb{N} \to \mathbb{R}^{\geq 0}$ is called *negligible* if for every $d > 0$ there exists some λ_0 such that for every $\lambda > \lambda_0$ it holds that $\varepsilon(\lambda) < \frac{1}{\lambda^d}$.

Definition 2.3. *(Computational indistinguishablity)* Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be efficiently sampleable distributions indexed by the security parameter λ. We say that $\boldsymbol{X}$ and $\boldsymbol{Y}$ are *computationally indistinguishable* and write $\boldsymbol{X}_\lambda \overset{c}{\equiv} \boldsymbol{Y}_\lambda$ if for every family of polynomial size circuits $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda \in \mathbb{N}}$ (i.e., $\mathcal{D}_\lambda$ has polynomially many gates in the security parameter), there exists a *negligible function* ε such that

$$|\Pr[\mathcal{D}_\lambda(\boldsymbol{X}_\lambda) = 1] - \Pr[\mathcal{D}_\lambda(\boldsymbol{Y}_\lambda) = 1]| \leq \varepsilon(\lambda) .$$

We usually drop the security parameter and write $\boldsymbol{X} \overset{c}{\equiv} \boldsymbol{Y}$ for $\boldsymbol{X}_\lambda \overset{c}{\equiv} \boldsymbol{Y}_\lambda$, and $\mathcal{D}(\boldsymbol{X}_\lambda)$ or $\mathcal{D}(\boldsymbol{X})$ instead of $\mathcal{D}_\lambda(\boldsymbol{X}_\lambda)$.

We will also face functions of the form $\varepsilon(n, \lambda)$, indexed by two parameters, which we require them to be polynomial in n and negligible in λ (e.g., to be of the form $\mathsf{poly}(n)\mathsf{negl}(\lambda)$), where n will be the number of participants in secret sharing schemes. To remove any confusion, we make the definition precise.

Definition 2.4. We say that, $\varepsilon(n, \lambda)$, where $\varepsilon : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{R}^{\geq 0}$, is polynomial in n and negligible in λ if for every $\lambda \in \mathbb{N}$, the function $\varepsilon'_\lambda(n) := \varepsilon(n, \lambda)$ is polynomial in n, and for every $n \in \mathbb{N}$, the function $\varepsilon''_n(\lambda) := \varepsilon(n, \lambda)$ is negligible in λ. An example of such a function is $n^2 \frac{1}{2^\lambda}$.

2.2. *One-Way Function*

Definition 2.5. *(OWF)* A function $f : \{0, 1\}^\star \to \{0, 1\}^\star$ is called a one-way function (OWF) if the following two conditions hold:

1. There is a polynomial-time algorithm that on input x outputs $f(x)$.
2. For every polynomial-size circuit family $\{\mathcal{C}_\lambda\}_\lambda$, the following probability is negligible:

$$\Pr[f(\mathcal{C}_\lambda(f(\boldsymbol{U}_\lambda))) = f(\boldsymbol{U}_\lambda)].$$

The following lemma is due to Impagliazzo, Levin, and Luby [17]. It was used by Impagliazzo and Luby in [18] to prove that short-key SKE implies OWF. In Sect. 4, we use this lemma, in a similar manner, to prove that computational RR-SSS for AC^0 implies the existence of OWF.

Lemma 2.6. ([17]) *If there is a polynomial-time computable function $f : \{0, 1\}^\lambda \to \{0, 1\}^{l(\lambda)}$, a polynomial-time samplable distribution $\boldsymbol{D} = \{\boldsymbol{D}_\lambda\}_\lambda$ and a constant $d > 0$ such that $f(\boldsymbol{U}_\lambda) \overset{c}{\equiv} \boldsymbol{D}_\lambda$ and for large enough λ, $H(\boldsymbol{D}_\lambda) \geq H(f(\boldsymbol{U}_\lambda)) + 1/\lambda^d$, then there is a OWF.*

2.3. *Access Structure*

In the secret sharing context, there is *set of participants*, which we denote by P, and a distinguished participant called the *dealer*, which we denote by $0 \notin P$.

Definition 2.7. *(Access structure)* A non-empty subset $\Gamma \subseteq 2^P$, with $\emptyset \notin \Gamma$, is called an *access structure* on P if it is *monotone*; that is, $A \subseteq B \subseteq P$ and $A \in \Gamma$ imply that that $B \in \Gamma$. A subset $A \subseteq P$ is called *qualified* if $A \in \Gamma$; otherwise, it is called *unqualified*. A qualified subset is called *minimal* if none of its proper subsets is qualified. An unqualified subset is called *maximal* if every proper superset of it is qualified.

There is a natural one-to-one correspondence between access structures with n participants and monotone Boolean functions with n variables.

2.4. *Secret Sharing*

A secret sharing scheme (SSS) can be defined in the following two equivalent ways. The first definition is more useful for working in the information-theoretic setting, while the second one is more useful in the computational setting.

Definition 2.8. *(SSS in terms of jointly distributed RVs)* A tuple $\left(\boldsymbol{S}_i\right)_{i \in P \cup \{0\}}$ of jointly distributed RVs is called a *SSS* on the set of participants P when $|\mathsf{supp}(\boldsymbol{S}_0)| \geq 2$. The RV $\boldsymbol{S}_0$ is called the *secret* RV and its support is called the *secret space*. The RV $\boldsymbol{S}_i$ is called the *share* RV of the participant $i \in P$ and its support is called his *share space*.

Definition 2.9. *(SSS in terms of sharing map)* Let $\mu : \mathcal{S}_0 \times \mathcal{R} \to \left(\mathcal{S}_i\right)_{i \in P}$ be a mapping and $\boldsymbol{R}$ be a distribution on $\mathcal{R}$, called the *randomness RV*. We refer to $\Pi = (\boldsymbol{R}, \mu)$ as a SSS if $|\mathcal{S}_0| \geq 2$. We call μ the *sharing map* and $\mathcal{R}$ the *randomness space*. Also, $\mathcal{S}_0$ is called the secret space and $\mathcal{S}_i$ is called the share space of participant i

The equivalence of these two definitions follows by the functional representation lemma (Lemma 2.1).

The following notation will be used throughout the paper.

Notation 2.10. *For a SSS $\Pi = \left(\boldsymbol{S}_i\right)_{i \in P \cup \{0\}}$ and a subset $A \subseteq P$, we use the notation $\boldsymbol{S}_A$ for the projection of Π on the components in A; i.e., $\boldsymbol{S}_A := \left(\boldsymbol{S}_i\right)_{i \in A}$. Also, for a sharing map $\mu : \mathcal{S}_0 \times \mathcal{R} \to \left(\mathcal{S}_i\right)_{i \in P}$, μ_A stands for the projection of μ on the components in A. That is, if $(s_i)_{i \in P} = \mu(s, r)$, then $\mu_A(s, r) := (s_i)_{i \in A}$.*

Linear SSS We call a SSS with sharing map $\mu : \mathcal{S}_0 \times \mathcal{R} \to \left(\mathcal{S}_i\right)_{i \in P}$ and randomness $\boldsymbol{R}$ *linear* when $\mathcal{R}$ and all $\mathcal{S}_i$'s, $i \in P \cup \{0\}$, are vector spaces over a common finite field, μ is a linear map and $\boldsymbol{R}$ is uniformly distributed over $\mathcal{R}$. Throughout the paper, for simplicity, we assume that he underline finite field is the binary field.

2.5. *Security Definitions for SSSs*

The security of a SSS can be defined both in information-theoretic and computational settings.

Definition 2.11. *(Perfect security)* We say that $\Pi = \big(\boldsymbol{S}_i\big)_{i \in P \cup \{0\}}$ is a *perfect SSS* for an access structure Γ, if the following two conditions hold:

- *Perfect correctness* $\mathrm{H}(\boldsymbol{S}_0 | \boldsymbol{S}_A) = 0$ for every qualified set $A \in \Gamma$.
- *Perfect privacy* $\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_B) = 0$ for every unqualified set $B \notin \Gamma$.

If Π is a perfect SSS for Γ, we also say that Π *realizes* Γ perfectly or Γ *admits* Π perfectly.

Computational secret sharing is defined to realize a family $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ of access structures, where Γ_n is an access structure with n participants with participants set P_n. A computational SSS for Γ is a tuple $\Pi = \big(\boldsymbol{R}, \mu\big)$ with

$$\boldsymbol{R} = \{\boldsymbol{R}_{\lambda,n}\}_{n,\lambda \in \mathbb{N}} \ ,$$
$$\mu = \{\mu_{\lambda,n} : \mathcal{S}_{0,\lambda,n} \times \mathcal{R}_{\lambda,n} \rightarrow \big(\mathcal{S}_{i,\lambda,n}\big)_{i \in P_n}\}_{\lambda,n \in \mathbb{N}} \ ,$$

where for every $\lambda, n \in \mathbb{N}$, the tuple $\big(\boldsymbol{R}_{\lambda,n}, \mu_{\lambda,n}\big)$ is a secret sharing scheme with participant set P_n. For simplicity, we drop the subscripts λ and n and simply say that $\Pi = \big(\boldsymbol{R}, \mu\big)$ with $\mu : \mathcal{S}_0 \times \mathcal{R} \rightarrow \big(\mathcal{S}_i\big)_{i \in P}$ is a family of SSSs indexed by λ and n. That is, we implicitly assume that all the components of the scheme (i.e., the sharing map, the secret, randomness, and share spaces and RVs) are indexed by λ and n.

Definition 2.12. *(Computational security)* Let $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ be a collection of access structures and $\Pi = \big(\boldsymbol{R}, \mu\big)$ with $\mu : \mathcal{S}_0 \times \mathcal{R} \rightarrow \big(\mathcal{S}_i\big)_{i \in P}$ be a family of SSSs indexed by the security parameter λ and n. We say that Π is a *computational SSS* for Γ if the following conditions hold:

- *Efficient randomness sampling* The RV $\boldsymbol{R}$ is polynomial-time sampleable in λ and n.
- *Polynomial secret length* $\log |\mathcal{S}_0|$ is polynomial in λ and n.
- *Efficient sharing* The sharing map μ is polynomial-time computable in λ and n.
- *Efficient secret reconstruction*There exists a polynomial-time algorithm Recon in λ and n such that for every qualified set $A \in \Gamma_n$ and secret $s \in \mathcal{S}_0$, the reconstruction error probability $\Pr[\mathsf{Recon}(A, \mu_A(s, \boldsymbol{R})) \neq s]$ is negligible in λ and polynomial in n (see Definition 2.4).
- *Computational privacy* for every unqualified set $B \notin \Gamma_n$ and every pair of secrets $s, s' \in \mathcal{S}_0$, $\mu_B(s, \boldsymbol{R}) \overset{c}{\equiv} \mu_B(s', \boldsymbol{R})$. Additionally, we require that the negligible function that exists for these two computationally indistinguishable distributions by Definition 2.3 be polynomial in n (see Definition 2.4).

Remark 2.13. Note that we do not restrict n to be a function of λ; because, if we do so, we have to change the access structure every time we change the security parameter, which is generally an undesirable property. Nevertheless, we will occasionally consider the case of $n = \mathsf{poly}(\lambda)$ towards proving some of our theoretical results. Also note that because n is an independent parameter, we have to parameterize the reconstruction error and distinguisher's advantage as functions of both n and λ. Nevertheless, we do not require them to be negligible in n (not even reverse polynomial in n). For our purposes, it suffices to require these quantities to be negligible in λ and polynomial in n (see Definition 2.4).

If Π is a computational SSS for $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$, we may simply say that Π is a computational SSS for Γ_n. We also say that Π *realizes* Γ_n computationally or Γ_n *admits* Π computationally.

The following lemma will be used later in the paper. Here, we present a sketch of the proof. We refer to Appendix A for the full proof.

Lemma 2.14. *Let $\Pi = (\mu, \mathbf{R})$ be a perfect/computational SSS with t-bit secrets and let $\boldsymbol{S}$ be an RV independent of $\mathbf{R}$ over the secret space. Then, for every unqualified set B,*

$$(\boldsymbol{S}, \mu_B(\boldsymbol{S}, \mathbf{R})) \overset{c}{\equiv} (\boldsymbol{S}, \mu_B(0^t, \mathbf{R})).$$

Proof. (Sketch) In the case of perfect SSS, the assertion immediately follows the independence of $\boldsymbol{S}$ and $\mu_B(\boldsymbol{S}, \mathbf{R})$. Assume that Π is a computational SSS. Let $\mathcal{D}$ be a polynomial-size circuit that distinguishes $(\boldsymbol{S}, \mu_B(\boldsymbol{S}, \mathbf{R}))$ and $(\boldsymbol{S}, \mu_B(0^t, \mathbf{R}))$ with non-negligable probability. Because $\mathbf{R}$ is independent of $\boldsymbol{S}$, there is a secret $s \in \mathsf{supp}(\boldsymbol{S})$ such that $\mathcal{D}$ distinguishes $(s, \mu_B(s, \mathbf{R}))$ and $(s, \mu_B(0^t, \mathbf{R}))$ with non-negligable probability. Let $\mathcal{C}(\cdot) = \mathcal{D}(s, \cdot)$. Then $\mathcal{C}$ distinguishes $\mu_B(s, \mathbf{R})$ and $\mu_B(0^t, \mathbf{R})$ with non-negligible probability which contradicts the computational privacy of the SSS. □

2.6. *Information Ratio*

The efficiency of SSSs is usually measured using a parameter called *information ratio*. The information ratio of an SSS with participants set P, secret space $\mathcal{S}_0$ and share space $\mathcal{S}_i$ for participant $i \in P$, is defined to be $\max_{i\in P} \frac{\log|\mathcal{S}_i|}{\log|\mathcal{S}_0|}$.

The *perfect information ratio*, or simply information ratio, of an access structure is defined to be the infimum of all information ratios of all SSSs that perfectly realize it.

Beimel [5] has conjectured that there are families of access structures with exponential information ratio in the number of participants; see Conjecture 1.2.

Remark 2.15. Beimel has also stated the conjecture in terms of *share size* instead of information ratio in [5]; this corresponds to the case where the secret is a single bit. There are access structures whose information ratio for exponentially-long secrets (in the number of participants) may be significantly better than the information ratio achievable for short secrets [3]. Nevertheless, it is widely believed that the stronger conjecture (i.e., for information ratio) holds true.

Csirmaz framework for lower bounding information ratio Following [11,25], Csirmaz proposed a framework in [12] to prove lower bounds on the information ratio of perfect

SSSs. His framework is captured in the following lemma which is based on the properties of the entropy function as well as the correctness and privacy properties of perfect SSSs.

Lemma 2.16. (Csirmaz/Perfect) *Let* $\Pi = (\boldsymbol{S}_i)_{i \in P \cup \{0\}}$ *be a perfect SSS for an access structure* Γ*. For every subset* $A \subseteq P \cup \{0\}$*, let* $f(A) = \frac{\mathrm{H}(\boldsymbol{S}_A)}{\mathrm{H}(\boldsymbol{S}_0)}$*. Then, the following holds:*

1. *Non-negativity* $f(A) \geq 0$ *for every* $A \subseteq P \cup \{0\}$.
2. *Monotonicity* $f(A) \geq f(B)$ *for every* $B \subseteq A \subseteq P \cup \{0\}$.
3. *Submodularity* $f(A) + f(B) \geq f(A \cup B) + f(A \cap B)$ *for every* $A, B \subseteq P \cup \{0, \}$.
4. *Strong monotonicity* $f(A) \geq f(B) + 1$ *for every* $A \in \Gamma$ *and* $B \subseteq A$ *such that* $B \notin \Gamma$.
5. *Strong submodularity* $f(A) + f(B) \geq f(A \cup B) + f(A \cap B) + 1$ *for every* $A, B \in \Gamma$ *such that* $A \cap B \notin \Gamma$.

If, using the inequalities (1.)–(5.), one can prove that for some participant $i \in P$, it holds that $f(\{i\}) \geq \sigma$, then σ will be a lower bound on the information ratio of the underlying access structure.

2.7. *Randomness Recoverable SSS*

We call a SSS $\Pi = (\boldsymbol{R}, \mu)$ *randomness recoverable (RR)* if qualified sets, in addition to the secret, can also recover the randomness; that is, there exists a function $\mathsf{RNDrecover}$ such that for every qualified set A, $\Pr[\mathsf{RNDrecover}(\mu_A(\boldsymbol{R}, s)) = \boldsymbol{R}] = 1$ for every secret s. When Π is a computational SSS, we require that $\mathsf{RNDrecover}$ be a polynomial-time algorithm, in the security parameter and the number of participants; we also allow a negligible amount of error; i.e., $\Pr[\mathsf{RNDrecover}(\mu_A(\boldsymbol{R}, s)) = \boldsymbol{R}]$ can be negligible in the security parameter and polynomial in the number of participants (see Definition 2.4 and Remark 2.13).

The following claim will be used in Sects. 3 and 4.

Claim 2.17. *If* $\Pi = (\boldsymbol{S}_i)_{i \in P \cup \{0\}}$ *is an RR-SSS with perfect correctness (i.e., zero reconstruction error probability), then for every pair of qualified sets* A, B*, we have* $\mathrm{H}(\boldsymbol{S}_A) = \mathrm{H}(\boldsymbol{S}_B)$*, or equivalently* $f(A) = f(B)$*, using the notation of Lemma 2.16.*

Proof. Denote the support of $\boldsymbol{S}_i$ by $\mathcal{S}_i$, for $i \in P \cup \{0\}$. Let $(\boldsymbol{R}, \mu)$, with $\mu : \mathcal{S}_0 \times \mathcal{R} \to \left(\mathcal{S}_i\right)_{i \in P}$, be the equivalent SSS in terms of Definition 2.9, which exists by the functional representation lemma (Lemma 2.1); that is, $\left(\boldsymbol{S}_0, (\boldsymbol{S}_i)_{i \in P}\right) \equiv \left(\boldsymbol{S}_0, \mu(\boldsymbol{S}_0, \boldsymbol{R})\right)$. For simplicity, let us assume that $(\boldsymbol{S}_i)_{i \in P} = \mu(\boldsymbol{S}_0, \boldsymbol{R})$. Since $\boldsymbol{S}_P$ is a function of the secret and randomness and every qualified set can recover both of them, it follows that $\mathrm{H}(\boldsymbol{S}_P | \boldsymbol{S}_A) = 0$, or equivalently $\mathrm{H}(\boldsymbol{S}_A) = \mathrm{H}(\boldsymbol{S}_P)$, for every qualified set A. The claim then follows. □

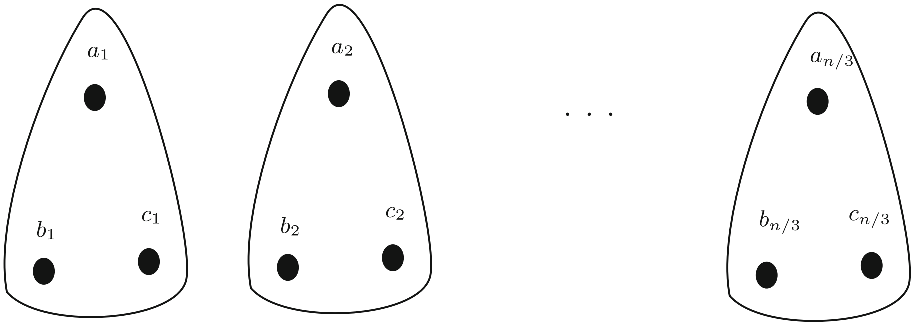


Fig. 2. The Moon-Moser access structure .

3. Exponential Lower Bound for Perfect RR-SSS

In this section, we show that the Moon-Moser access structure, to be defined below, has an exponential information ratio for every perfect RR-SSS that realizes it. The result also applies to weaker security notions such as statistical security as will be discussed at the end of this section.

The Moon-Moser access structure Due to an old result by Moon and Moser [33], any graph with n vertices has at most $3^{n/3}$ maximal independent sets. A graph with exactly $3^{n/3}$ maximal independent sets is easy to construct: simply take the disjoint union of $n/3$ triangle graphs. Motivated by this example, we consider the access structure in Fig. 2, which is the union of $n/3$ (3, 3)-threshold access structures, and refer to it as the Moon-Moser access structure. Clearly, this access structure lies in AC^0.

Theorem 3.1. *For every n, there is an access structure in AC^0 such that every perfect RR-SSS that realizes it has information ratio $2^{\Omega(n)}$.*

We first present a notation and a claim and then prove the theorem.

Notation Denote the set of participants of the Moon-Moser access structure, with n participants, by $P = \{a_1, b_1, c_1, \ldots, a_{n/3}, b_{n/3}, c_{n/3}\}$, with $\{a_i, b_i, c_i\}$ be a minimally qualified set for every $i = 1, \ldots, n/3$ (see Fig. 2). Let $\Pi = (\boldsymbol{S}_i)_{i \in P\cup\{0\}}$ be a perfect RR-SSS for this access structure and f be as in Lemma 2.16. For a participant $p_i \in \{a_i, b_i, c_i\}$, we define p'_i and p''_i to be the cyclic rotations of p_i by one and two positions, respectively; i.e., $a''_i = b'_i = c_i$, $b''_i = c'_i = a_i$ and $c''_i = a'_i = b_i$. Also, we denote a set $\{p_{i_1}, \ldots, p_{i_k}\}$ simply by $p_{i_1} \cdots p_{i_k}$.

Claim 3.2. *For every qualified set A, every $k = 0, 1, \ldots, n/3$, and all choices for $p_1, \ldots, p_k$ with $p_i \in \{a_i, b_i, c_i\}$, the following inequality holds:*

$$f(A) \geq f(p_1 p'_1 \ldots p_k p'_k) + 3^{n/3-k} \ . \tag{3.1}$$

Proof of Claim 3.2. First, let us show that the following inequality is implied by Inequality (3.1):

$$f(A) \geq f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k) + 2 \times 3^{n/3-k} . \tag{3.2}$$

By Inequality (3.1) we have:

$$f(A) \geq f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k p'_k) + 3^{n/3-k} ,$$
$$f(A) \geq f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p''_k p_k) + 3^{n/3-k} .$$

Also by the monotonicity property, we have

$$f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k p'_k) + f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p''_k p_k) \geq$$
$$f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k p'_k p''_k) + f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k) .$$

Notice that $p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k p'_k p''_k$ is qualified and, hence, by Claim 2.17 we have

$$f(A) = f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k p'_k p''_k)$$

. Therefore, Inequality (3.2) follows by adding the above three inequalities.

Now, we prove Inequality (3.1) by backward induction on k.

Base Denote $m = n/3$. For $k = m$, by strong submodularity property, we have:

$$f(p''_1 p_1 p'_1 \ldots p_m p'_m) + f(p''_2 p_1 p'_1 \ldots p_m p'_m) \geq f(p''_1 p''_2 p_1 p'_1 \ldots p_m p'_m)$$
$$+ f(p_1 p'_1 \ldots p_m p'_m) + 1 .$$

Since the sets $p''_1 p_1 p'_1 \ldots p_m p'_m$, $p''_2 p_1 p'_1 \ldots p_m p'_m$ and $p''_1 p''_2 p_1 p'_1 \ldots p_m p'_m$ are all qualified, for every qualified set A, by Claim 2.17, we have:

$$f(A) = f(p''_1 p_1 p'_1 \ldots p_m p'_m) = f(p''_2 p_1 p'_1 \ldots p_m p'_m) = f(p''_1 p''_2 p_1 p'_1 \ldots p_m p'_m) .$$

Therefore,

$$f(A) \geq f(p_1 p'_1 \ldots p_m p'_m) + 1 ;$$

that is, Inequality (3.1) holds for $k = n/3$.

Induction Now suppose that by the induction hypothesis

$$f(A) \geq f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p_k p'_k) + 3^{n/3-k} .$$

By Inequality (3.2), we also have:

$$f(A) \geq f(p_1 p'_1 \ldots p_{k-1} p'_{k-1} p''_k) + 2 \times 3^{n/3-k} .$$

By the monotonicity property, we have

$$f(p_1p_1'\dots p_{k-1}p_{k-1}'p_kp_k') + f(p_1p_1'\dots p_{k-1}p_{k-1}'p_k'') \geq \\ f(p_1p_1'\dots p_{k-1}p_{k-1}'p_kp_k'p_k'') + f(p_1p_1'\dots p_{k-1}p_{k-1}') \,.$$

By adding the above three inequalities, noticing that $p_1p_1'\dots p_{k-1}p_{k-1}'p_kp_k'p_k''$ is qualified, and using Claim 2.17, we get:

$$f(A) \geq f(p_1p_1'\dots p_{k-1}p_{k-1}') + 3^{n/3-(k-1)} \,;$$

that is, Inequality (3.1) holds for $k-1$. This completes the proof of Claim 3.2. □

Proof of Theorem 3.1. Let $p_i \in \{a_1, b_1, c_1, \dots, a_{n/3}, b_{n/3}, c_{n/3}\}$. By letting $k = 0$ and $A = \{p_i, p_i', p_i''\}$ in Inequality (3.1), we have:

$$f(p_ip_i'p_i'') \geq 3^{n/3} \,.$$

Also, $f(p_i) + f(p_i') + f(p_i'') \geq f(p_ip_i'p_i'')$. Therefore, for every $i \in \{1, \dots, n/3\}$, for at least one $p \in \{a_i, b_i, c_i\}$, we have

$$f(p) \geq 3^{n/3-1} \,. \qquad \square$$

Remark 3.3. The above proof can be converted, in a straightforward manner, to a proof for the case of an access structure that is the union of n/k disjoint (k, k)-thresholds. Stated explicitly, every perfect RR-SSS that realizes the access structure that has

$$\{a_{1,1}, a_{1,2}, \cdots, a_{1,k}\}, \{a_{2,1}, a_{2,2}, \cdots, a_{2,k}\}, \cdots, \{a_{n/k,1}, a_{n/k,2}, \cdots, a_{n/k,k}\}$$

as its minimal qualified sets has information-ratio $2^{\Omega(n \log k/k)}$. The best exponent is achieved for $k = 3$, which justifies our choice for the Moon-Moser access structure in this section.

Exponential lower bound for non-perfect RR-SSSs Besides perfect and computational security, several non-perfect security notions for secret sharing have appeared in the literature, including *almost-perfect*, *quasi-perfect*, and *statistical*. We refer to [21] for a comprehensive study of these security notions. Kaced [22, Theorem 36] has shown that any lower bound derived on the information ratio of (standard) SSSs using information inequalities applies not only to perfect security but also to quasi-perfect security (which can be shown to apply to almost-perfect and statistical security too). His result can also be extended to the case of RR-SSSs. Since, we only used (Shannon-type) information inequalities to derive our exponential lower bound on perfect RR-SSS, it also holds for all mentioned non-perfect security notions.

4. Computational RR-SSS for AC^0 Implies OWF

In this section, we show that the existence of computational RR-SSS for some access structures in AC^0 implies the existence of OWFs. Our method is similar to Impagliazzo and Levin's method for proving that short-key SKE implies OWFs [18]. The idea is as follows: if $\Pi = (\mu, \boldsymbol{R})$ is a SSS for an access structure where B is unqualified, then $\boldsymbol{S}||\mu_B(\boldsymbol{S}, \boldsymbol{R})$ and $\boldsymbol{S}'||\mu_B(\boldsymbol{S}, \boldsymbol{R})$ are computationally indistinguishable, where $\boldsymbol{S}$ and $\boldsymbol{S}'$ are independent uniform RVs over the secret space. Indeed, when the SSS is perfect, $\mu_B(\boldsymbol{S}, \boldsymbol{R})$ reveals no information about $\boldsymbol{S}$ and so the two distributions are information-theoretically indistinguishable. But when the SSS is computational, $\mu_B(\boldsymbol{S}, \boldsymbol{R})$ reveals some information about $\boldsymbol{S}$. If this amount is not negligible, then we have two distributions that are computationally indistinguishable but statistically distinguishable and we can apply Lemma 2.6 to deduce the existence of OWF.

In Sect. 3, it was shown that there are access structures in AC^0 that do not admit efficient perfect RR-SSSs. In other words, an RR-SSS for such an access structure, that perfectly hides the secret from unqualified sets, has to have shares with exponential length. Hence intuitively, in a computational RR-SSS for such an access structure (because shares are of polynomial length), there are unqualified sets that obtain a considerable amount of *information* about the secret. This intuition is exactly phrased and proved in this section.

For simplicity, we first study the simpler case where in the definition of computational SSS (Definition 2.12), we require the reconstruction error probability to be equal to zero.

4.1. *Zero Reconstruction Error*

In this subsection, we present a lemma, a claim, and a corollary for computational SSSs with zero reconstruction errors. These results are modified in Sect. 4.2 to consider non-zero reconstruction error and will be used in Sect. 4.3 to prove the main result of this section.

A variant of Csirmaz's framework (see lemma 2.16) adapted to the computational setting with perfect correctness (i.e., zero reconstruction error) is needed. The following lemma states this variant.

Lemma 4.1. (Csirmaz/Computational/Perfect correctness) *Let* $\Pi = (\boldsymbol{S}_i)_{i\in P\cup\{0\}}$ *be a computational SSS with perfect correctness for an access structure* Γ. *For* $A, B \subseteq P \cup \{0\}$, *denote* $H(\boldsymbol{S}_A)$ *with* $H(A)$ *and* $H(\boldsymbol{S}_A|\boldsymbol{S}_B)$ *with* $H(A|B)$, *respectively. Then, the non-negativity, monotonicity, and submodularity properties hold as in Lemma 2.16 and, one has the following modified formulation of strong monotonicity and strong submodularity:*

1. *Strong monotonicity* $H(A) \geq H(B) + H(0|B)$ *for every* $A \in \Gamma$ *and* $B \subset A$ *such that* $B \notin \Gamma$.
2. *Strong submodularity* $H(A) + H(B) \geq H(A \cup B) + H(A \cap B) + H(0|A \cap B)$ *for every* $A, B \in \Gamma$ *such that* $A \cap B \notin \Gamma$.

Proof. Inequality (1) holds because A is qualified and due to the monotonicity property:

$$H(A) = H(\{0\} \cup A) \geq H(\{0\} \cup B) = H(B) + H(0|B).$$

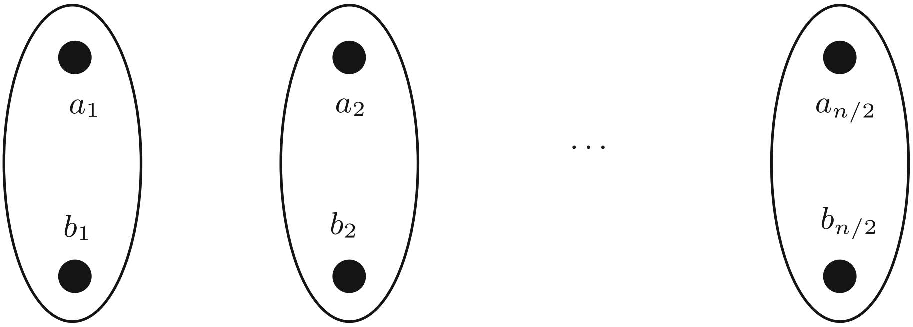


Fig. 3. Union of (2, 2)-threshholds .

Inequality (2) follows from the following relations:

$$\begin{aligned} H(A) + H(B) &= H(\{0\} \cup A) + H(\{0\} \cup B) \\ &\geq H(\{0\} \cup A \cup B) + H(\{0\} \cup (A \cap B)) \\ &\geq H(A \cup B) + H(A \cap B) + H(0|A \cap B). \end{aligned}$$

In the first equality, we have used the fact that A and B are qualified. The first and second inequalities follow by the submodularity and monotonicity properties, respectively.

□

Notation In what follows, let $P = \{a_1, b_1, a_2, b_2, \cdots, a_{n/2}, b_{n/2}\}$ and Γ be an access structure with minimally qualified sets $\{a_1, b_1\}, \cdots, \{a_{n/2}, b_{n/2}\}$ (see Fig. 3). Note that this access structure lies in AC^0. According to Remark 3.3, Γ's information ratio is $2^{\Omega(n)}$. For $p_i \in \{a_i, b_i\}$, let p'_i be the other element of $\{a_i, b_i\}$; i.e., if $p_i = a_i$ then $p'_i = b_i$ and if $p_i = b_i$ then $p'_i = a_i$. Also denote $\{p_1, p_2, \cdots, p_k\}$ with $p_1 p_2 \cdots p_k$ and use the notation in Lemma 4.1 for entropies.

Claim 4.2. *Let Π be a computational RR-SSS with perfect correctness for Γ and A be a qualified set in Γ with $H(A) \leq c$. Then for all $k = 0, 1, \cdots, n/2$,*

$$H(\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_k) + \frac{c}{2^k} \geq H(A),$$

where $\boldsymbol{p}_i$ is a uniform RV over $\{a_i, b_i\}$ and $\boldsymbol{p}_i$'s are independent.

Proof. We prove the claim by induction on k. *Base:* The base ($k = 0$) holds by the assumption. *Induction:* Suppose that by the induction hypothesis we have:

$$H(\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_k) + \frac{c}{2^k} \geq H(A), \tag{4.1}$$

where $k < n/2$. By the submodularity property

$$H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k a_{k+1}) + H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k b_{k+1}) \geq H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k a_{k+1} b_{k+1}) + H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k). \tag{4.2}$$

Since $\{\boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_k, a_{k+1}, b_{k+1}\}$ is qualified, then according to Claim 2.17, we have:

$$H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k a_{k+1} b_{k+1}) = H(A). \tag{4.3}$$

Summing up relations (4.1), (4.2) and (4.3), we get:

$$H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k a_{k+1}) + H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k b_{k+1}) + \frac{c}{2^k} \geq 2H(A).$$

So:

$$H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k\boldsymbol{p}_{k+1}) + \frac{c}{2^{k+1}} = \frac{1}{2}\big(H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k a_{k+1}) + H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_k b_{k+1})\big) + \frac{c}{2^{k+1}} \geq H(A)\ .$$

□

The following corollary could be considered as a quantitative contrapositive for Theorem 3.1.

Corollary 4.3. *Let Π be a computational RR-SSS for Γ with perfect correctness and m-bit secrets and let n be a polynomial in λ. Then for large enough λ:*

$$\frac{m}{2} \geq H(0|\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}),$$

where $\boldsymbol{p}_i$ is a uniform RV over $\{a_i, b_i\}$ and $\boldsymbol{p}_i$'s are independent.

Proof. Sharing algorithm's running time and m are polynomials, so for large enough λ we have $2^{\frac{n}{2}-1}m \geq H(A)$, where A is an arbitrary qualified set. Applying Claim 4.2 to this inequality, if follows that

$$H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}) + \frac{m}{2} \geq H(A). \tag{4.4}$$

On the other hand, $\{\boldsymbol{p}'_1, \boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_{n/2}\}$ and $\{\boldsymbol{p}'_2, \boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_{n/2}\}$ are qualified sets, while $\{\boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_{n/2}\}$ is not. So, according to the (computational) strong submodularity property,

$$H(\boldsymbol{p}'_1\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}) + H(\boldsymbol{p}'_2\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}) \geq H(\boldsymbol{p}'_1\boldsymbol{p}'_2\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}) + H(\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}) + H(0|\boldsymbol{p}_1\boldsymbol{p}_2\cdots\boldsymbol{p}_{n/2}).$$

Applying Claim 2.17, we get

$$H(A) \geq H(\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_{n/2}) + H(0|\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_{n/2}).$$

Summing up the above inequality and Inequality (4.4), one gets the desired result. □

4.2. *Non-zero Reconstruction Error*

In this subsection, we provide variants of Lemma 4.1, Claim 4.2, and Corollary 4.3 that do not assume zero reconstruction error.

When the reconstruction error is zero, the entropy of the secret conditioned on the share of a qualified set is zero, because in this case, the secret is determined by the qualified set's share. When we allow the reconstruction algorithm to fail with some bounded probability, this property no longer holds. The following is a variant of Fano's inequality that we will use to prove that in this case, conditioned on the share of a qualified set, the entropy of the secret is $o(1)$.

Lemma 4.4. *Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be families of RVs such that $\boldsymbol{Y}$ has polynomial length and f be a function such that $\Pr[\boldsymbol{Y} \neq f(\boldsymbol{X})]$ is negligible. Then $H(\boldsymbol{Y}|\boldsymbol{X})$ is $o(1)$.*

Proof. Define the indicator RV $\boldsymbol{Z}$ as follows:

$$\boldsymbol{Z} = \begin{cases} 1 \text{ if } \boldsymbol{Y} = f(\boldsymbol{X}) \\ 0 \text{ if } \boldsymbol{Y} \neq f(\boldsymbol{X}) \end{cases} .$$

Since $H(\boldsymbol{Z}|\boldsymbol{X}, \boldsymbol{Y}) = 0$, we have:

$$\begin{aligned} H(\boldsymbol{Y}|\boldsymbol{X}) &= H(\boldsymbol{Y}|\boldsymbol{X}) + H(\boldsymbol{Z}|\boldsymbol{X}, \boldsymbol{Y}) \\ &= H(\boldsymbol{Y}, \boldsymbol{Z}|\boldsymbol{X}) \\ &= H(\boldsymbol{Z}|\boldsymbol{X}) + H(\boldsymbol{Y}|\boldsymbol{X}, \boldsymbol{Z}) \\ &\leq H(\boldsymbol{Z}) + \sum_{x \in \mathsf{Supp}(\boldsymbol{X})} \big(\Pr[\boldsymbol{X} = x, \boldsymbol{Z} = 0] H(\boldsymbol{Y}|\boldsymbol{X} = x, \boldsymbol{Z} = 0) \\ &\quad + \Pr[\boldsymbol{X} = x, \boldsymbol{Z} = 1] H(\boldsymbol{Y}|\boldsymbol{X} = x, \boldsymbol{Z} = 1)\big) \\ &= o(1) + \sum_{x \in \mathsf{Supp}(\boldsymbol{X})} \Pr[\boldsymbol{X} = x, \boldsymbol{Z} = 0] H(\boldsymbol{Y}|\boldsymbol{X} = x, \boldsymbol{Z} = 0) \quad (4.5) \\ &\leq o(1) + \left(\sum_{x \in \mathsf{Supp}(\boldsymbol{X})} \Pr[\boldsymbol{X} = x, \boldsymbol{Z} = 0] \right) \log(|\mathsf{Supp}(\boldsymbol{Y})|) \quad (4.6) \\ &= o(1) + \Pr[\boldsymbol{Z} = 0] \log(|\mathsf{Supp}(\boldsymbol{Y})|) \\ &= o(1). \quad (4.7) \end{aligned}$$

Equation (4.5) holds for two reasons: First, $\boldsymbol{Z}$ is a Bernouli RV with $\Pr[\boldsymbol{Z} = 0] = o(1)$ (indeed, this probability is negligable), so $H(\boldsymbol{Z}) = o(1)$; Second, when $\boldsymbol{Z} = 1$, $\boldsymbol{Y}$ is determined by $\boldsymbol{X}$; therefore, $H(\boldsymbol{Y}|\boldsymbol{X}=x,\boldsymbol{Z}=1)=0$. Inequality (4.6) holds because $H(\boldsymbol{Y})\le\log(|\mathsf{Supp}(\boldsymbol{Y})|)$. Equality (4.7) holds because $\Pr[\boldsymbol{Z}=0]$ is negligable and $\boldsymbol{Y}$ has polynomial length. □

Lemma 4.5. *Let $\Pi=(\mu,\boldsymbol{R})$ be a computational SSS, n be a polynomial in λ and $\boldsymbol{S}_0$ be an RV over the secret space. Then for every qualified set A, $H(\boldsymbol{S}_0|\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))=o(1)$.*

Proof. Let Recon be the reconstruction algorithm and $\delta=\delta(\lambda,n)$ be the reconstruction error. Then $\Pr[\mathsf{Recon}(A,\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))\neq\boldsymbol{S}_0]\le\delta(\lambda,n)$ and because n is a polynomial in λ, this probability is negligable. Also, the length of $\boldsymbol{S}_0$ is polynomial. Therefore, according to Lemma 4.4, $H(\boldsymbol{S}_0|\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))=o(1)$.

□

The following is a variant of Claim 2.17 that does not assume zero reconstruction error.

Claim 4.6. *Let $\Pi=(\mu,\boldsymbol{R})$ be a computational RR-SSS, n be a polynomial in λ and $\boldsymbol{S}_0$ be an RV over the secret space. Then for any two qualified sets A and B, $|H(\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))-H(\mu_B(\boldsymbol{S}_0,\boldsymbol{R}))|=o(1)$.*

Proof. By Lemma 4.5, $H(\boldsymbol{S}_0|\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))=o(1)$. Because Π is RR, it can be proved that similarly

$$H(\boldsymbol{R}|\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))=o(1).$$

Therefore, $H(\boldsymbol{S}_0,\boldsymbol{R}|\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))=o(1)$ and, hence, $H(\boldsymbol{S}_0,\boldsymbol{R})\le H(\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))+o(1)$. On the other hand, $\mu_A(\boldsymbol{S}_0,\boldsymbol{R})$ is determined by $\boldsymbol{S}_0$ and $\boldsymbol{R}$; thus $H(\mu_A(\boldsymbol{S}_0,\boldsymbol{R}))\le H(\boldsymbol{S}_0,\boldsymbol{R})$. Similar bounds hold for $\mu_B(\boldsymbol{S}_0,\boldsymbol{R})$. The claim follows from these bounds. □

The following is a variant of Csirmaz's computational framework (4.1) stated for the case of the non-zero reconstruction error.

Lemma 4.7. (Csirmaz/Computational) *Let $\Pi=(\boldsymbol{S}_i)_{i\in P\cup\{0\}}$ be a computational SSS for an access structure Γ and n be a polynomial in λ. Then, the non-negativity, monotonicity, and submodularity properties hold as in Lemma 2.16 and, one has the following modified formulation of strong monotonicity and strong submodularity:*

1. *Strong monotonicity $H(A)+o(1)\ge H(B)+H(0|B)$ for every $A\in\Gamma$ and $B\subset A$ such that $B\notin\Gamma$.*
2. *Strong submodularity $H(A)+H(B)+o(1)\ge H(A\cup B)+H(A\cap B)+H(0|A\cap B)$ for every $A,B\in\Gamma$ such that $A\cap B\notin\Gamma$.*

Proof. Inequality (1) follows from the following relations:

$$H(A)+o(1)=H(\{0\}\cup A)\ge H(\{0\}\cup B)=H(B)+H(0|B).$$

The left-hand side equality follows from Lemma 4.6. The rest is as in the proof of Lemma 4.1. Inequality (2) follows from the following relations:

$$\begin{aligned} H(A) + H(B) + o(1) &= H(\{0\} \cup A) + H(\{0\} \cup B) \\ &\geq H(\{0\} \cup A \cup B) + H(\{0\} \cup (A \cap B)) \\ &\geq H(A \cup B) + H(A \cap B) + H(0|A \cap B). \end{aligned}$$

The equality follows from Lemma 4.6. The rest is as in the proof of Lemma 4.1. □

Below is a modification of Claim 4.2 stated for the case of the non-zero reconstruction error.

Claim 4.8. *Let Π be a computational RR-SSS for Γ, n be a polynomial in λ and A be a qualified set such that $H(A) \leq c$. Then for $k = 0, 1, \cdots, n/2$ one has:*

$$H(\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_k) + \frac{c}{2^k} + o(1) \geq H(A),$$

where $\boldsymbol{p}_i$ is a uniform RV over $\{a_i, b_i\}$ and $\boldsymbol{p}_i$'s are independent.

Proof. Proof of this claim is achieved by applying appropriate and straightforward modifications to the proof of Claim 4.2. Explicitly, Claim 2.17 is used there to deduce $H(\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_k a_{k+1} b_{k+1}) = H(A)$. Instead, we apply Claim 4.6 to deduce

$$H(\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_k a_{k+1} b_{k+1}) + o(1) \geq H(A).$$

Also, the induction hypothesis should be modified to include the term $o(1)$. □

Finally, we state a variant of Corollary 4.3 that does not assume zero reconstruction error.

Corollary 4.9. *Let Π be a computational RR-SSS for Γ with m-bit secrets and n be a polynomial in λ. Then*

$$\frac{m}{2} + o(1) \geq H(0|\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_{n/2}),$$

where $\boldsymbol{p}_i$ is a uniform RV over $\{a_i, b_i\}$ and $\boldsymbol{p}_i$'s are independent.

Proof. The proof is the same as the proof of Corollary 4.3 with the following exceptions: Usages of Claim 4.2 and Claim 2.17 are replaced with those of Claim 4.8 and Claim 4.6, respectively. Indeed, these replacements substitute each claim with a corresponding variant that is adapted to the case of the non-zero reconstruction error. Also, the variant of strong submodularity that is stated in Lemma 4.7 should be used. □

4.3. *Main Result*

Theorem 4.10. *Let Γ be the union of $n/2$ disjoint $(2, 2)$-thresholds (see Fig. 3). If Γ has a computational RR-SSS, then there exists an OWF.*

Proof. As in the previous subsections, assume that $\{a_i, b_i\}$, $1 \leq i \leq n/2$, are the minimal qualified sets. Let $\Pi = (\mu, \boldsymbol{R})$ be a computational RR-SSS for Γ with m-bit secrets and $n = \mathsf{poly}(\lambda)$. For $0 \leq i \leq n/2$, take $\boldsymbol{p}_i$ to be a uniform RV over $\{a_i, b_i\}$ and set $\boldsymbol{B} = \{\boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_{n/2}\}$.

According to Corollary 4.9 we have,

$$\frac{m}{2} + o(1) \geq H(0|\boldsymbol{p}_1 \boldsymbol{p}_2 \cdots \boldsymbol{p}_{n/2}).$$

So if we let $\boldsymbol{S}_0$ be a uniform RV over the secret space, then

$$\frac{m}{2} + o(1) + H(\mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})) \geq H(\boldsymbol{S}_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})).$$

Let $\boldsymbol{S}'_0$ be a uniform secret independent of $\boldsymbol{S}_0$ and $\boldsymbol{R}$. Then

$$H(\boldsymbol{S}'_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})) = m + H(\mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})).$$

These together imply that

$$H(\boldsymbol{S}'_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})) + o(1) \geq H(\boldsymbol{S}_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})) + \frac{m}{2}. \tag{4.8}$$

On the other hand, because $(\boldsymbol{S}_0, \boldsymbol{R})$ and $(\boldsymbol{S}'_0, \boldsymbol{R})$ have the same distribution, we have $\boldsymbol{S}_0 || \mu_B(\boldsymbol{S}_0, \boldsymbol{R}) \overset{c}{\equiv} \boldsymbol{S}'_0 || \mu_B(\boldsymbol{S}'_0, \boldsymbol{R})$. Also it follows from the computational privacy of the SSS that $\boldsymbol{S}'_0 || \mu_B(\boldsymbol{S}_0, \boldsymbol{R}) \overset{c}{\equiv} \boldsymbol{S}'_0 || \mu_B(\boldsymbol{S}'_0, \boldsymbol{R})$. Putting these together, we get

$$\boldsymbol{S}'_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R}) \overset{\text{c}}{\equiv} \boldsymbol{S}_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R}). \tag{4.9}$$

Applying Lemma 2.6 to (4.8) and (4.9) (with $\boldsymbol{D}_\lambda = \boldsymbol{S}'_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})$ and $f(\boldsymbol{S}_0 || \boldsymbol{R} || \boldsymbol{B}) = \boldsymbol{S}_0 || \mu_{\boldsymbol{B}}(\boldsymbol{S}_0, \boldsymbol{R})$), we get the desired result. □

5. Construction of Computational RR-SSS

In this section, we observe that computational RR-SSS for NC^1 can be based on simple minicrypt primitives that have some kind of one-time KDM-like security. In particular, we first observe that an efficient linear SSS (and generally, an efficient SSS with a property that we call *randomness simulatability*) can be converted into a computational RR-SSS assuming the existence of one-time KDM-secure RR-SKE. Next we introduce the notion of *linear-resistant* PRG. Then, we see how an efficient perfect linear SSS can be converted into an efficient computational RR-SSS, using a linear-resistant PRG.

5.1. *RR-SKE and KDM Security*

First, we recall the definition of (RR-)SKE and (one-time) KDM-security.

Definition 5.1. (SKE/RR-SKE) Let $\mathcal{M} = \{\mathcal{M}_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of message spaces and $\Sigma = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a tuple of probabilistic polynomial-time algorithms where

- Gen, called key-generation algorithm, on input 1^λ returns a key k,
- Enc, called encryption algorithm, gets a message m and a key k as input and returns a ciphertext ct,
- Dec, called decryption algorithm, gets a ciphertext ct and a key k as input and returns a message m or $\perp$.

Σ is called a symmetric-key encryption (SKE) for $\mathcal{M}$ if for every $m \in \mathcal{M}_\lambda$:

$$\Pr[k \leftarrow \mathsf{Gen}(1^\lambda); ct \leftarrow \mathsf{Enc}_k(m) : \mathsf{Dec}_k(ct) = m] = 1 .$$

We call Σ randomness recoverable SKE (RR-SKE) if additionally there exists a polynomial-time algorithm $\mathsf{Recover}$ such that:

$$\Pr[k \leftarrow \mathsf{Gen}(1^\lambda); ct \leftarrow \mathsf{Enc}_k(m; \boldsymbol{R}) : \mathsf{Recover}_k(ct) = \boldsymbol{R}] = 1 ,$$

where $\boldsymbol{R}$ is the randomness used in the encryption algorithm.

Definition 5.2. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an SKE with key-space $\mathcal{K}$ and message-space $\mathcal{M}$. We say that Π is one-time KDM-secure, if for each efficiently computable function $f : \mathcal{K} \to \mathcal{M}$,

$$\{k \leftarrow \mathsf{Gen}(1^\lambda) : \mathsf{Enc}_k(f(k))\} \overset{c}{\equiv} \{k \leftarrow \mathsf{Gen}(1^\lambda) : \mathsf{Enc}_k(0^{|f(k)|})\}.$$

The standard construction of Symmetric-Key Encryption (SKE) based on a pseudorandom function is RR. In the next section, we will discuss SKE schemes that ensure both randomness recoverability and one-time KDM-security. The work of [27] surveys RR-SKE schemes that meet KDM-security criteria for projection functions (simple functions where each output bit is dependent on only one input bit). Additionally, the research by [2] demonstrates how to extend KDM-security from projection functions to general efficient functions. However, this transformation does not maintain the randomness recoverability. To the best of our knowledge, RR-SKE schemes that satisfy one-time KDM-security for general efficient functions have not yet been addressed in the literature.

Lemma 5.3. *Assume that* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is a one-time KDM-secure SKE and* $g : \{0, 1\}^{l_1+l_2+l_3} \to \{0, 1\}^l$ *is an effieciently computable function. Then one has*

$$(\mathbf{x}, \mathsf{Enc}_{\boldsymbol{k}}(g(\boldsymbol{k}, \mathbf{x}, \mathbf{y}))) \overset{c}{\equiv} (\mathbf{x}, \mathsf{Enc}_{\boldsymbol{k}}(0^l))$$

where $\boldsymbol{k}$ *is* Π*'s key and has length* l_1 *and* $(\mathbf{x}, \mathbf{y})$ *are jointy distributed RVs over* $\{0, 1\}^{l_2} \times \{0, 1\}^{l_3}$ *and independent of* $\boldsymbol{k}$.

Here, we present a sketch of the proof. We refer to Appendix B for the full proof.

Proof. (Sketch) Let $\mathcal{D}$ be a polynomial-size circuit that distinguishes the distributions $(\mathbf{x}, \mathsf{Enc}_{\boldsymbol{k}}(0^l))$ and $(\mathbf{x}, \mathsf{Enc}_{\boldsymbol{k}}(g(\boldsymbol{k}, \mathbf{x}, \mathbf{y})))$ with non-negligable probability. Because $\boldsymbol{k}$ is independent of $(\mathbf{x}, \mathbf{y})$, there are $(x, y) \in \mathsf{supp}(\mathbf{x}) \times \mathsf{supp}(\mathbf{y})$ such that $\mathcal{D}$ distinguishes $(x, \mathsf{Enc}_{\boldsymbol{k}}(g(\boldsymbol{k}, x, y)))$ and $(x, \mathsf{Enc}_{\boldsymbol{k}}(0^l))$. Let $\mathcal{C}(\cdot) = \mathcal{D}(x, \cdot)$ and $f(\cdot) = g(\cdot, x, y)$. Then $\mathcal{C}$ distinguishes $\mathsf{Enc}_{\boldsymbol{k}}(f(\boldsymbol{k}))$ and $\mathsf{Enc}_{\boldsymbol{k}}(0^l)$ with non-negligible probability which is in contradiction with the KDM security of Π. □

5.2. *RR-SSS from Randomness Simulatable SSS and One-Time KDM-Secure RR-SKE*

Consider this simple construction for a computational RR-SSS using a general (i.e., not necessarily perfect or linear) efficient standard SSS (which is known to exist for access structures in mP, assuming OWF) and an RR-SKE with one-time KDM-security. The construction is as follows. First, use the SSS to share $s||k$ with randomness r to compute the shares for the secret s, where k is the key of the SKE. Then, encrypt r under the secret key k using the SKE and append the ciphertext to the shares. The correctness and randomness recoverability requirements are trivial. Privacy follows from the KDM-security of the SKE. However, in order for the proof to go through, we require a property of the original SSS that we refer to as the *randomness simulatability*. Every linear SSS has this property but it remains open whether every access structure in mP admits a randomness simulatable SSS.

In the following, we first define the notion of *randomness simulatable* SSS. Then, we present a theorem that formalizes the above construction.

Definition 5.4. *(Randomness simulatable SSS)* Let $\Pi = (\boldsymbol{R}, \mu)$ be a perfect or computational SSS for an access structure. We say that SSS Π is *randomness simulatable*, if for each RV $\boldsymbol{S}$ over the secret space and each unqualified set B there exists an efficiently computable function g and an efficiently sampleable RV $\widehat{\boldsymbol{R}}$ independent of $(\boldsymbol{S}, \boldsymbol{R})$ such that

$$(\boldsymbol{S}, \boldsymbol{\mu}_B, \boldsymbol{R}) \overset{c}{\equiv} (\boldsymbol{S}, \boldsymbol{\mu}_B, g(\boldsymbol{S}, \boldsymbol{\mu}_B, \widehat{\boldsymbol{R}})) ,$$

where $\boldsymbol{\mu}_B = \mu_B(\boldsymbol{S}, \boldsymbol{R})$ denotes the share of the unqualified set B.

Notice that, ignoring the efficient computability of g and efficient sampleability of $\widehat{\boldsymbol{R}}$, the existence of g and $\widehat{\boldsymbol{R}}$ is always guaranteed by the functional representation lemma (Lemma 2.1). Also, in particular, linear SSSs are randomness simulatable. It is unclear to us whether every access structure in mP —which is known to admit an efficient computational SSS [40] (see also [38])—admits a randomness simulatable scheme.

Theorem 5.5. *Let Π be a one-time KDM-secure RR-SKE with ℓ-bit keys. Let μ_i be the sharing map of the i'th participant in a perfect/computational randomness simulatable SSS for an access structure with t-bit secret, $t > \lambda$, and ρ-bit randomness (i.e., the share of participant i is $\mu_i(s, r)$, where s is the secret and r is the randomness).*

Then, the SSS defined below is a computational RR-SSS for the same access structure.

Given a secret $s \in \{0,1\}^{t-\ell}$ and a randomness $r \in \{0,1\}^{\rho}$:

- *generate a key $k \leftarrow \mathsf{Gen}(1^{\lambda})$,*
- *let $ct \leftarrow \mathsf{Enc}_k(r)$,*
- *let $\mu_i(s||k, r)||ct$ be the share of i'th participant.*

Proof. Correctness and randomness recoverability trivially hold. We prove privacy. Let $s \in \{0,1\}^{t-\ell}$ be an arbitrary secret and let B be an unqualified set in the access structure. Let $\boldsymbol{R}$ be SSS's randomness, $\boldsymbol{k}$ denote $\mathsf{Gen}(1^{\lambda})$ and $\boldsymbol{\mu}_B$ denote $\mu_B(s||\boldsymbol{k}, \boldsymbol{R})$. For ease of notation, we simply denote the share of B for the secret s by $\boldsymbol{\mu}_B||\mathsf{Enc}_{\boldsymbol{k}}(\boldsymbol{R})$ (i.e., we ignore the repetitions of $\mathsf{Enc}_{\boldsymbol{k}}(\boldsymbol{R})$). Based on the randomness simulatability of the SSS, there exists an efficiently computable function g and an efficiently sampleable RV $\widehat{\boldsymbol{R}}$ independent of $(\boldsymbol{k}, \boldsymbol{R})$ such that

$$(s||\boldsymbol{k}, \boldsymbol{\mu}_B, \boldsymbol{R}) \stackrel{c}{\equiv} (s||\boldsymbol{k}, \boldsymbol{\mu}_B, g(s||\boldsymbol{k}, \boldsymbol{\mu}_B, \widehat{\boldsymbol{R}}))$$

Therefore, one has the following indistinguishability:

$$\boldsymbol{\mu}_B||\mathsf{Enc}_{\boldsymbol{k}}(\boldsymbol{R}) \stackrel{c}{\equiv} \boldsymbol{\mu}_B||\mathsf{Enc}_{\boldsymbol{k}}(g(s||\boldsymbol{k}, \boldsymbol{\mu}_B, \widehat{\boldsymbol{R}})) \tag{5.1}$$

According to Lemma 2.14, one has

$$(\boldsymbol{k}, \mu_B(s||\boldsymbol{k}, \boldsymbol{R})) \stackrel{c}{\equiv} (\boldsymbol{k}, \mu_B(0^t, \boldsymbol{R})).$$

In other words, $(\boldsymbol{k}, \boldsymbol{\mu}_B) \stackrel{c}{\equiv} (\boldsymbol{k}, \boldsymbol{\mu}'_B)$, where $\boldsymbol{\mu}'_B = \mu_B(0^t, \boldsymbol{R})$. Because g is efficiently computable and $\widehat{\boldsymbol{R}}$ is efficiently sampleable and independent of $(\boldsymbol{k}, \boldsymbol{R})$, we have

$$\boldsymbol{\mu}_B||\mathsf{Enc}_{\boldsymbol{k}}(g(s||\boldsymbol{k}, \boldsymbol{\mu}_B, \widehat{\boldsymbol{R}})) \stackrel{c}{\equiv} \boldsymbol{\mu}'_B||\mathsf{Enc}_{\boldsymbol{k}}(g(s||\boldsymbol{k}, \boldsymbol{\mu}'_B, \widehat{\boldsymbol{R}})). \tag{5.2}$$

On the other hand, because $(\boldsymbol{\mu}'_B, \widehat{\boldsymbol{R}})$ is independent of $\boldsymbol{k}$, by Lemma 5.3, we have:

$$\boldsymbol{\mu}'_B||\mathsf{Enc}_{\boldsymbol{k}}(g(s||\boldsymbol{k}, \boldsymbol{\mu}'_B, \widehat{\boldsymbol{R}})) \stackrel{c}{\equiv} \boldsymbol{\mu}'_B||\mathsf{Enc}_{\boldsymbol{k}}(0^l). \tag{5.3}$$

Equations (5.1), (5.2) and (5.3) then imply that

$$\boldsymbol{\mu}_B||\mathsf{Enc}_{\boldsymbol{k}}(\boldsymbol{R}) \stackrel{c}{\equiv} \boldsymbol{\mu}'_B||\mathsf{Enc}_{\boldsymbol{k}}(0^l)\ .$$

Because $\boldsymbol{\mu}'_B||\mathsf{Enc}_{\boldsymbol{k}}(0^l)$ hides the secret s, privacy follows. □

5.3. *Linear-Resistant PRG*

In this section, we present a variant of pseudo-random generators (PRG), with a KDM-like security for the class of linear functions.

Recall that a polynomial-time deterministic algorithm, $G : \{0,1\}^\star \to \{0,1\}^\star$ that maps λ-bit strings to $\ell(\lambda)$-bit strings is said to be PRG if $\ell(\lambda) > \lambda$ and $G(\boldsymbol{U}_\lambda) \overset{c}{\equiv} \boldsymbol{U}_{\ell(\lambda)}$.

In the following definition, $\{0,1\}$ is identified with $\mathbb{F}_2$, the finitie field with two elements, and $+$ stands for the addition in the field or bitwise-XOR; that is, for $x = x_1, \dots, x_\ell$ and $y = y_1, \dots, y_\ell$, $x + y = (x_1 \oplus y_1)|| \cdots ||(x_\ell \oplus y_\ell)$.

Definition 5.6. Let $G : \{0,1\}^\lambda \to \{0,1\}^\ell$ be a polynomial-time deterministic algorithm with $\ell := \ell(\lambda) > \lambda$. We call G a *linear-resistant* PRG if for every $\mathbb{F}_2$-linear function $L : \{0,1\}^\lambda \to \{0,1\}^\ell$, $G(\boldsymbol{U}_\lambda) + L(\boldsymbol{U}_\lambda) \overset{c}{\equiv} \boldsymbol{U}_\ell$.

Clearly, every linear-resistant PRG is also a PRG. However, the converse is not necessarily correct. For example, if $G : \{0,1\}^{\lambda-1} \to \{0,1\}^{\ell-1}$ is a PRG, then so is $G' : \{0,1\}^\lambda \to \{0,1\}^\ell$ defined as $G'(s_1 \cdots s_\lambda) = s_1||G(s_2 \cdots s_\lambda)$. It is clear that G' is not linear-resistant.

It is easy to see that linear-resistant PRG implies one-time KDM-secure SKE against the class of all affine functions: simply consider the standard one-time-pad encryption scheme $\mathsf{Enc}_k(m) = G(k) + m$. More precisely, if the input and output lengths of the linear-resistant PRG G are λ and ℓ, the key and message spaces of the constructed scheme are $\mathcal{K} = \mathbb{F}_2^\lambda$ and $\mathcal{M} = \mathbb{F}_2^\ell$, respectively, and it has KDM-security against all affine functions from $\mathbb{F}_2^\lambda$ to $\mathbb{F}_2^\ell$.

In particular, since this scheme is deterministic, the resulting SKE is RR.

Another variant of PRG that has a KDM-like property is the hinting PRG which can be used to achieve one-time KDM-secure SKE against any class of functions that can be computed in fixed polynomial time [27, Appendix B]. Also, note that both of these primitives can be instantiated using a random oracle. Despite the similarity between linear-resistant PRG and hinting PRG, the relationship between these primitives remains open, as is the (im)possibility of constructing linear-resistant PRG from OWF. In contrast, black-box separation between hinting PRG and PKE is known [1].

5.4. *RR-SSS from Linear Perfect SSS and Linear-Resistant PRG*

Consider the following simple construction for a computational RR-SSS using an efficient (standard) linear perfect SSS and a linear-resistant PRG G. To share a secret s, use the linear SSS to share $s||r$ with randomness $G(r)$ to compute the shares, where r is the randomness. It is clear that every qualified set can recover not only s but also r. Privacy follows from the linear-resistance security of the PRG. Notice that the class of access structures that admit efficient linear SSS is equivalent to the class of monotone boolean functions that admit efficient MSP (monotone-span programs [24]) which includes NC^1 (e.g., using the Benaloh-Leichter [8] construction).

We state the above construction in a theorem:

Theorem 5.7. *Let μ be the sharing map of a perfect linear SSS for an access structure with $k\lambda$-bit secrets, $k > 1$, and ℓ-bit randomness (i.e., the shares of participants are the outputs of $\mu(s, r)$, where s is the secret and r is the randomness). Let $G : \{0, 1\}^{\lambda} \to \{0, 1\}^{\ell}$ be a linear-resistant PRG. Then, the SSS defined by the sharing map $\mu'(s, r) = \mu(s||r, G(r))$ is a computational RR-SSS for the same access structure, where $s \in \{0, 1\}^{(k-1)\lambda}$ is the secret and $r \in \{0, 1\}^{\lambda}$ is the randomness with uniform distribution.*

Proof. Correctness and randomness recoverability trivially hold. We prove privacy. Let B be an unqualified set and let $\mu_B(s_1||s_2, r) = L_1(s_1) + L_2(s_2) + L_3(r)$ be the share of B for the secret $s_1||s_2$ and randomness $r \in \{0, 1\}^{\ell}$ in the perfect linear scheme, where L_i's are linear functions, $s_1 \in \{0, 1\}^{(k-1)\lambda}$ and $s_2 \in \{0, 1\}^{\lambda}$.

By perfect privacy of the linear scheme, for any $s \in \{0, 1\}^{(k-1)\lambda}$, the RVs $L_2(s)+L_3(\boldsymbol{r})$ and $L_3(\boldsymbol{r})$ have the same distributions, where $\boldsymbol{r}$ is a uniform RVs on ℓ-bit strings (they correspond to the shares of the secrets $s||0^{\lambda}$ and $0^{k\lambda}$, respectively). Therefore $\mathsf{supp}(L_2(s) + L_3(\boldsymbol{r})) = \mathsf{supp}(L_3(\boldsymbol{r}))$ which implies that $L_2(s) + \mathsf{range}(L_3) = \mathsf{range}(L_3)$. As a result $L_2(s) \in \mathsf{range}(L_3)$ and because s is arbitrary, we have $\mathsf{range}(L_2) \subseteq \mathsf{range}(L_3)$. If f and g are linear functions from V to W such that range of g is a subspace of the range of f, then for a suitable linear function h over V one has $g = f \circ h$. By this fact, there is a linear function L such that $L_2 = L_3 \circ L$.

Let $s, s' \in \{0, 1\}^{(k-1)\lambda}$ be two arbitrary secrets and $\boldsymbol{r}$ be as before. Again, by perfect privacy of the linear scheme, $L_1(s) + L_3(\boldsymbol{r})$ and $L_1(s') + L_3(\boldsymbol{r})$ have the same distributions (they correspond to the shares of the secrets $s||0^{\lambda}$ and $s'||0^{\lambda}$, respectively). Since G is linear-resistant, by a standard reduction argument, $L_1(s) + L_3(G(\boldsymbol{r}) + L(\boldsymbol{r}))$ and $L_1(s') + L_3(G(\boldsymbol{r}) + L(\boldsymbol{r}))$ are computationally indistinguishable where $\boldsymbol{r}$ is a uniform RV on λ-bit strings. Therefore, $\mu'_B(s, \boldsymbol{r}) = L_1(s) + L_2(\boldsymbol{r}) + L_3(G(\boldsymbol{r}))$ and $\mu'_B(s', \boldsymbol{r}) = L_1(s') + L_2(\boldsymbol{r}) + L_3(G(\boldsymbol{r}))$ are computationally indistinguishable, which is the desired result. □

We conclude this section with the following remark that relates the observations of this section and the previous ones.

Remark 5.8. Notice that in the proof of Theorem 5.5, we do not require that the SKE be KDM-secure against the whole class of efficiently computable functions. Indeed, security against all the functions g for all unqualified sets is sufficient. Since the class of linear SSSs is randomness simulatable with linear g's, and one-time secure RR-SKE against the class of linear functions is implied by linear-resistant PRG, Theorem 5.7 follows by Theorem 5.5, via a simpler construction though.

6. Conclusion

We initiated the study of SSS from the viewpoint of randomness recovery. By proving an exponential lower bound for the information ratio of an RR-SSS that realizes some very simple access structure in monotone AC^0, we showed that the situation is very different for RR-SSS, compared to the standard SSS, for which the best-known lower bound is sub-linear. We also managed to shed some light on the complexity of the computational RR-SSS, by proving that computational RR-SSS for certain access structures in monotone AC^0 implies OWF. This computational result is essentially a consequence of our information-theoretic lower bound; This can be justified by the very general idea that an algorithm that hides the secret from a bounded adversary but is unable to do so against an unbounded adversary implies OWF.

In the final section, we observed that an efficient perfect linear SSS can be converted into a computational RR-SSS for the same access structure using a type of PRG that we called linear-resistant PRG. We also noted that using a one-time KDM-secure RR-SKE, one can convert an efficient perfect/computational SSS into an RR-SSS, assuming that the SSS has the extra property of randomness simulatability.

Acknowledgements

We would like to thank Sorush Bahariyan for bringing Fact 1 to our attention and Motahareh Gharahi for fruitful discussions on the proof of Theorem 3.1. We also extend our gratitude to the anonymous reviewers for their time and valuable feedback.

A. Full Proof of Lemma 2.14

In the case of perfect SSS, the assertion immediately follows the independence of $\boldsymbol{S}$ and $\mu_B(\boldsymbol{S}, \mathbf{R})$. Assume that Π is a computational SSS, $\mathbf{R} = \{\mathbf{R}_\lambda\}_\lambda$, $\boldsymbol{S} = \{\boldsymbol{S}_\lambda\}_\lambda$ and $t = t(\lambda)$. For contradiction, let poly be a polynomial and $\mathcal{D} = \{\mathcal{D}_\lambda\}_\lambda$ be a family of polynomial-size distinguishers such that for infinitely many λ,

$$|\Pr[\mathcal{D}_\lambda(\boldsymbol{S}_\lambda, \mu_B(\boldsymbol{S}_\lambda, \mathbf{R}_\lambda)) = 1] - \Pr[\mathcal{D}_\lambda(\boldsymbol{S}_\lambda, \mu_B(0^{t(\lambda)}, \mathbf{R}_\lambda)) = 1]| \geq \frac{1}{\mathsf{poly}(\lambda)}.$$

Therefore, for each λ, there is $s_\lambda \in \mathsf{supp}(\mathsf{s}_\lambda)$ such that

$$|\Pr[\mathcal{D}_\lambda(s_\lambda, \mu_B(s_\lambda, \mathbf{R}_\lambda)) = 1] - \Pr[\mathcal{D}_\lambda(s_\lambda, \mu_B(0^{t(\lambda)}, \mathbf{R}_\lambda)) = 1]| \geq \frac{1}{\mathsf{poly}(\lambda)}.$$

Therefore, for $\mathcal{C}_\lambda(\cdot) = \mathcal{D}_\lambda(s_\lambda, \cdot)$ one has

$$|\Pr[\mathcal{C}_\lambda(\mu_B(s_\lambda, \mathbf{R}_\lambda)) = 1] - \Pr[\mathcal{C}_\lambda(\mu_B(0^{t(\lambda)}, \mathbf{R}_\lambda)) = 1]| \geq \frac{1}{\mathsf{poly}(\lambda)} ,$$

which contradicts the computational privacy of the SSS.

B. Full Proof of Lemma 5.3

Let $\boldsymbol{k} = \{\boldsymbol{k}_\lambda\}_\lambda$ where $\boldsymbol{k}_\lambda = \mathsf{Gen}(1^\lambda)$, $\mathbf{x} = \{\mathbf{x}_\lambda\}_\lambda$, $\mathbf{y} = \{\mathbf{y}_\lambda\}_\lambda$ and $g = \{g_\lambda\}_\lambda$. Assume that the assertion is false and there is a polynomial poly and a polynomial-size distinguisher $D = \{\mathcal{D}_\lambda\}_\lambda$ and infinitely many λ for which:

$$|\Pr[\mathcal{D}_\lambda(\mathbf{x}_\lambda, \mathsf{Enc}_{\boldsymbol{k}_\lambda}(g_\lambda(\boldsymbol{k}_\lambda, \mathbf{x}_\lambda, \mathbf{y}_\lambda))) = 1] - \Pr[\mathcal{D}_\lambda(\mathbf{x}_\lambda, \mathsf{Enc}_{\boldsymbol{k}_\lambda}(0^{l(\lambda)})) = 1]| \geq \frac{1}{\mathsf{poly}(\lambda)}.$$

Because $\boldsymbol{k}$ is independent of $\mathbf{x}$ and $\mathbf{y}$, for each such λ, there is $(x_\lambda, y_\lambda) \in \mathsf{supp}(\mathbf{x}_\lambda) \times \mathsf{supp}(\mathbf{y}_\lambda)$ such that:

$$|\Pr[\mathcal{D}_\lambda(x_\lambda, \mathsf{Enc}_{\boldsymbol{k}_\lambda}(g_\lambda(\boldsymbol{k}_\lambda, x_\lambda, y_\lambda))) = 1] - \Pr[\mathcal{D}_\lambda(x_\lambda, \mathsf{Enc}_{\boldsymbol{k}_\lambda}(0^{l(\lambda)})) = 1]| \geq \frac{1}{\mathsf{poly}(\lambda)}.$$

Letting $\mathcal{C}_\lambda(\cdot) = \mathcal{D}_\lambda(x_\lambda, \cdot)$ and $f_\lambda(\cdot) = g_\lambda(\cdot, x_\lambda, y_\lambda)$, we have

$$|\Pr[\mathcal{C}_\lambda(\mathsf{Enc}_{\boldsymbol{k}_\lambda}(f_\lambda(\boldsymbol{k}_\lambda))) = 1] - \Pr[\mathcal{C}_\lambda(\mathsf{Enc}_{\boldsymbol{k}_\lambda}(0^{l(\lambda)})) = 1]| \geq \frac{1}{\mathsf{poly}(\lambda)},$$

which contradicts the KDM-security of Π.

References

[1] N. Alamati, S. Patranabis, Cryptographic primitives with hinting property. In S. Agrawal, D. Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part I*, volume 13791 of *Lecture Notes in Computer Science* (Springer, 2022), pp. 33–62.

[2] B. Applebaum, Key-dependent message security: Generic amplification and completeness. *J. Cryptol.* **27**(3):429–451 (2014)

[3] B. Applebaum, B. Arkis, On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. *ACM Trans. Comput. Theory* **12**(4):241–2421 (2020)

[4] B. Applebaum, A. Beimel, Y. Ishai, E. Kushilevitz, T. Liu, V. Vaikuntanathan, Succinct computational secret sharing, in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023 (Association for Computing Machinery, 2023), pp. 1553-1566

[5] A. Beimel, Secret-sharing schemes: A survey, in *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, pp. 11–46, 2011.

[6] A. Beimel, Y. Ishai, On the power of nonlinear secret-sharing. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001* (2001), pp. 188–202

[7] M. Bellare, P. Rogaway, Optimal asymmetric encryption. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science* (Springer, 1994), pp. 92–111

[8] J. C. Benaloh, J. Leichter, Generalized secret sharing and monotone functions, in *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings* (1988), pp. 27–35

[9] G. R. Blakley, Safeguarding cryptographic keys, in *Proceedings of the 1979 AFIPS National Computer Conference* (1979) vol. 48, pp. 313–317

[10] D. Boneh, Simplified OAEP for the RSA and rabin functions. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA,*

August 19-23, 2001, Proceedings, volume 2139 of *Lecture Notes in Computer Science* (Springer, 2001), pp. 275–291

[11] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares for secret sharing schemes. *J. Cryptol.* **6**(3):157–167 (1993)

[12] L. Csirmaz. The size of a share must be large. *J. Cryptol.* **10**(4):223–231 (1997)

[13] L. Csirmaz, Secret sharing and duality. *J. Math. Cryptol.* **15**(1):157–173 (2020)

[14] A. El Gamal, Y.-H. Kim, in *Network Information Theory*. Cambridge University Press (2011)

[15] S. Garg, M. Hajiabadi, G. Malavolta, R. Ostrovsky, How to build a trapdoor function from an encryption scheme. In M. Tibouchi and H. Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part III*, volume 13092 of *Lecture Notes in Computer Science* (Springer, 2021), pp. 220–249

[16] S. Hohenberger, V. Koppula, B. Waters, Chosen ciphertext security from injective trapdoor functions. In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part I*, volume 12170 of *Lecture Notes in Computer Science* (Springer, 2020), pp. 836–866

[17] R. Impagliazzo, L. A. Levin, M. Luby, Pseudo-random generation from one-way functions (extended abstracts). In D. S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA* (ACM, 1989), pp. 12–24.

[18] R. Impagliazzo, M. Luby, One-way functions are essential for complexity based cryptography, in *30th Annual Symposium on Foundations of Computer Science* (1989), pp. 230–235

[19] M. Ito, A. Saio, T. Nishizeki, Multiple assignment scheme for sharing secret. *J. Cryptol.* **6**(1):15–20 (1993)

[20] M. Ito, A. Saito, T. Nishizeki, Secret sharing scheme realizing general access structure. *Electron. Commun. Jpn.* **72**(9):56–64 (1989)

[21] A. Jafari, S. Khazaei, Partial secret sharing schemes. *IACR Cryptol. ePrint Arch.* 2020:448 (2020)

[22] T. Kaced, in *Secret Sharing and Algorithmic Information Theory. (Partage de secret et the'orie algorithmique de l'information)*. PhD thesis, Montpellier 2 University, France (2012)

[23] T. Kaced, Information inequalities are not closed under polymatroid duality. *IEEE Trans. Inf. Theory* **64**(6):4379–4381 (2018)

[24] M. Karchmer, A. Wigderson, On span programs, in *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18–21, 1993* (1993), pp. 102–111

[25] E. D. Karnin, J. W. Greene, M. E. Hellman, On secret sharing systems. *IEEE Trans. Inf. Theory* **29**(1):35–41 (1983)

[26] S. Khazaei, T. Moran, D. Wikström, A mix-net from any CCA2 secure cryptosystem. In X. Wang and K. Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science* (Springer, 2012), pp. 607–625

[27] F. Kitagawa, T. Matsuda, K. Tanaka. CCA security and trapdoor functions via key-dependent-message security. *J. Cryptol.* **35**(2):9 (2022)

[28] I. Komargodski, M. Naor, E. Yogev, Secret-sharing for NP. *J. Cryptol.* **30**(2):444–469 (2017)

[29] V. Koppula, B. Waters, Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. In A. Boldyreva, D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science* (Springer, 2019), pp. 671–700

[30] C. Ki Li, D. S. Wong, Signcryption from randomness recoverable public key encryption. *Inf. Sci.* **180**(4):549–559 (2010)

[31] A. Lombardi, W. Quach, R. D. Rothblum, D. Wichs, D. J. Wu, New constructions of reusable designated-verifier nizks. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*, volume 11694 of *Lecture Notes in Computer Science* (Springer, 2019), pp. 670–700

[32] S. Micali, Simple and fast optimistic protocols for fair electronic exchange. In E. Borowsky, S. Rajsbaum, editors, *Proceedings of the Twenty-Second ACM Symposium on Principles of Distributed Computing, PODC 2003, Boston, Massachusetts, USA, July 13-16, 2003* (ACM, 2003), pp. 12–19

[33] J. W. Moon, L. Moser, On cliques in graphs. *Israel J. Math.* **3**(1):23–28 (1965)

[34] D. H. Phan, D. Pointcheval, Chosen-ciphertext security without redundancy. In C.-S. Laih, editor, *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings*, volume 2894 of *Lecture Notes in Computer Science* (Springer, 2003), pp. 1–18

[35] P. Rogaway, M. Bellare, Robust computational secret sharing and a unified account of classical secret-sharing goals, in *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007* (2007), pp. 172–184

[36] A. Shamir, How to share a secret. *Commun. ACM* **22**(11):612–613 (1979)

[37] V. Shoup, OAEP reconsidered. *J. Cryptol.* **15**(4):223–249 (2002)

[38] V. Vaikuntanathan, A. Narayanan, K. Srinathan, C. Pandu Rangan, K. Kim, On the power of computational secret sharing. In T. Johansson and S. Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings*, volume 2904 of *Lecture Notes in Computer Science* (Springer, 2003), pp. 162–176

[39] A. C.-C. Yao, Theory and applications of trapdoor functions (extended abstract), in *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982* (IEEE Computer Society, 1982), pp. 80–91

[40] A. C.-C. Yao, Unpublished manuscript, presented at oberwolfach and dimacs workshops (1989)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.